

L Number	Hits	Search Text	DB	Time stamp
1	232	CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm	USPAT; EPO; JPO; DERWENT	2004/10/28 12:35
2	9818	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and 713/\$.ccls. or 380/\$.ccls.	USPAT; EPO; JPO; DERWENT	2004/10/28 10:48
3	20686	713/\$.ccls. or 380/\$.ccls.	USPAT; EPO; JPO; DERWENT	2004/10/28 10:48
4	10	( 713/\$.ccls. or 380/\$.ccls.) and (CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm)	USPAT; EPO; JPO; DERWENT	2004/10/28 11:50
5	23838	(deriv\$4 or generat\$4 or creat\$4) near4 offset	USPAT; EPO; JPO; DERWENT	2004/10/28 11:51
6	13589	(message or data or information or file) near3 (transformation)	USPAT; EPO; JPO; DERWENT	2004/10/28 11:53
7	29877	(lookup or mapping or map\$4 or array\$4) and (iterat\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 11:54
8	207	permutat\$5 same offset\$5	USPAT; EPO; JPO; DERWENT	2004/10/28 11:55
9	31207	second near4 transform\$5	USPAT; EPO; JPO; DERWENT	2004/10/28 11:56
12	11	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5))	USPAT; EPO; JPO; DERWENT	2004/10/28 11:57
13	5	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and ((message or data or information or file) near3 (transformation))	USPAT; EPO; JPO; DERWENT	2004/10/28 11:57
14	10	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and ((deriv\$4 or generat\$4 or creat\$4) near4 offset)	USPAT; EPO; JPO; DERWENT	2004/10/28 11:57
15	10	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and (( 713/\$.ccls. or 380/\$.ccls.) and (CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm))	USPAT; EPO; JPO; DERWENT	2004/10/28 11:57
16	10	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and ( 713/\$.ccls. or 380/\$.ccls.)	USPAT; EPO; JPO; DERWENT	2004/10/28 11:57
17	4	((deriv\$4 or generat\$4 or creat\$4) near4 offset) and ((message or data or information or file) near3 (transformation)) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5)) and (permutat\$5 same offset\$5) and (second near4 transform\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:20
10	9	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and (second near4 transform\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:00
11	8	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and (permutat\$5 same offset\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:01
19	807	380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls.	USPAT; EPO; JPO; DERWENT	2004/10/28 12:14
20	986	455/410-411.ccls.	USPAT; EPO; JPO; DERWENT	2004/10/28 12:02
21	1668	(380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls.) or 455/410-411.ccls.	USPAT; EPO; JPO; DERWENT	2004/10/28 12:03

22	7	((380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls.) or 455/410-411.ccls.) and (CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:03
23	10	tbox and ( 713/\$.ccls. or 380/\$.ccls.)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:09
24	5	((deriv\$4 or generat\$4 or creat\$4) near4 offset) and ((message or data or information or file) near3 (transformation)) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5)) and (permutat\$5 same offset\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:11
25	1486	380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.	USPAT; EPO; JPO; DERWENT	2004/10/28 12:14
26	21	(380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.) and ((deriv\$4 or generat\$4 or creat\$4) near4 offset)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:14
27	7	(380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.) and (CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:15
28	2346	(380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.) or 455/410-411.ccls.	USPAT; EPO; JPO; DERWENT	2004/10/28 12:15
29	22	((380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.) or 455/410-411.ccls.) and ((deriv\$4 or generat\$4 or creat\$4) near4 offset)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:15
30	134	((380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.) or 455/410-411.ccls.) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5))	USPAT; EPO; JPO; DERWENT	2004/10/28 12:15
31	134	((380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.) or 455/410-411.ccls.) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5))) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5))	USPAT; EPO; JPO; DERWENT	2004/10/28 12:15
32	6	((380/255.ccls. or 380/247.ccls. or 380/270.ccls. or 380/274.ccls. or 380/281.ccls. or 380/284.ccls. or 380/28.ccls.) or 455/410-411.ccls.) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5))) and (permutat\$5 same offset\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:16
33	0	block near2 cipher\$4 and (CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:20
34	1058	block near2 cipher\$4	USPAT; EPO; JPO; DERWENT	2004/10/28 12:20

35	0	((deriv\$4 or generat\$4 or creat\$4) near4 offset) and ((message or data or information or file) near3 (transformation)) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5)) and (permutat\$5 same offset\$5) and block near2 cipher	USPAT; EPO; JPO; DERWENT	2004/10/28 12:21
36	92073	block adj2 cipher\$4 or symmetric or secret	USPAT; EPO; JPO; DERWENT	2004/10/28 12:21
37	16	(CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm) and (block adj2 cipher\$4 or symmetric or secret)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:25
38	494	WEP or (CMEA or cellular adj1 message adj1 message adj1 encrypt\$5 adj1 algorithm)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:33
39	233	CMEA or cellular adj1 message adj1 encrypt\$5 adj1 algorithm	USPAT; EPO; JPO; DERWENT	2004/10/28 12:35
40	10	(CMEA or cellular adj1 message adj1 encrypt\$5 adj1 algorithm) and ((deriv\$4 or generat\$4 or creat\$4) near4 offset)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:35
41	5	(CMEA or cellular adj1 message adj1 encrypt\$5 adj1 algorithm) and ((message or data or information or file) near3 (transformation))	USPAT; EPO; JPO; DERWENT	2004/10/28 12:35
42	11	(CMEA or cellular adj1 message adj1 encrypt\$5 adj1 algorithm) and ((lookup or mapping or map\$4 or array\$4) and (iterat\$5))	USPAT; EPO; JPO; DERWENT	2004/10/28 12:35
43	8	(CMEA or cellular adj1 message adj1 encrypt\$5 adj1 algorithm) and (permutat\$5 same offset\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:36
44	9	(CMEA or cellular adj1 message adj1 encrypt\$5 adj1 algorithm) and (second near4 transform\$5)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:36
45	17	(CMEA or cellular adj1 message adj1 encrypt\$5 adj1 algorithm) and (block adj2 cipher\$4 or symmetric or secret)	USPAT; EPO; JPO; DERWENT	2004/10/28 12:36

SYSTEM: OS - DIALOG OneSearch

File 2: INSPEC 1969-2004/Oct W3  
(c) 2004 Institution of Electrical Engineers

**\*File 2: Alert feature enhanced for multiple files, duplicates removal, customized scheduling. See HELP ALERT.**

File 6: NTIS 1964-2004/Oct W2  
(c) 2004 NTIS, Intl Cpyrght All Rights Res  
File 8: Ei Compendex(R) 1970-2004/Oct W3  
(c) 2004 Elsevier Eng. Info. Inc.  
File 34: SciSearch(R) Cited Ref Sci 1990-2004/Oct W4  
(c) 2004 Inst for Sci Info  
File 434: SciSearch(R) Cited Ref Sci 1974-1989/Dec  
(c) 1998 Inst for Sci Info  
File 35: Dissertation Abs Online 1861-2004/Sep  
(c) 2004 ProQuest Info&Learning  
File 62: SPIN(R) 1975-2004/Aug W4  
(c) 2004 American Institute of Physics  
File 99: Wilson Appl. Sci & Tech Abs 1983-2004/Sep  
(c) 2004 The HW Wilson Co.  
File 144: Pascal 1973-2004/Oct W3  
(c) 2004 INIST/CNRS  
File 94: JICST-EPlus 1985-2004/Sep W4  
(c) 2004 Japan Science and Tech Corp(JST)  
File 233: Internet & Personal Comp. Abs. 1981-2003/Sep  
(c) 2003 EBSCO Pub.

**\*File 233: File 233 is closed (no longer updating).**

File 266: FEDRIP 2004/Aug  
Comp & dist by NTIS, Intl Copyright All Rights Res  
File 15: ABI/Inform(R) 1971-2004/Oct 28  
(c) 2004 ProQuest Info&Learning

**\*File 15: Alert feature enhanced for multiple files, duplicate removal, customized scheduling. See HELP ALERT.**

File 16: Gale Group PROMT(R) 1990-2004/Oct 28  
(c) 2004 The Gale Group

**\*File 16: Alert feature enhanced for multiple files, duplicate removal, customized scheduling. See HELP ALERT.**

File 98: General Sci Abs/Full-Text 1984-2004/Sep  
(c) 2004 The HW Wilson Co.  
File 239: Mathsci 1940-2004/Dec  
(c) 2004 American Mathematical Society  
File 275: Gale Group Computer DB(TM) 1983-2004/Oct 28  
(c) 2004 The Gale Group  
File 621: Gale Group New Prod. Annou. (R) 1985-2004/Oct 28  
(c) 2004 The Gale Group  
File 636: Gale Group Newsletter DB(TM) 1987-2004/Oct 28  
(c) 2004 The Gale Group  
File 647: CMP Computer Fulltext 1988-2004/Oct W3  
(c) 2004 CMP Media, LLC  
File 674: Computer News Fulltext 1989-2004/Sep W1  
(c) 2004 IDG Communications  
File 256: TecInfoSource 82-2004/Jul  
(c) 2004 Info.Sources Inc  
File 9: Business & Industry(R) Jul/1994-2004/Oct 27  
(c) 2004 The Gale Group  
File 148: Gale Group Trade & Industry DB 1976-2004/Oct 15  
(c) 2004 The Gale Group

**\*File 148: Alert feature enhanced for multiple files, duplicate removal, customized scheduling. See HELP ALERT.**

File 624: McGraw-Hill Publications 1985-2004/Oct 28  
(c) 2004 McGraw-Hill Co. Inc

**\*File 624: Homeland Security & Defense and 9 Platt energy journals added**  
Please see HELP NEWS624 for more

File 553: Wilson Bus. Abs. FullText 1982-2004/Sep  
(c) 2004 The HW Wilson Co  
File 696: DIALOG Telecom. Newsletters 1995-2004/Oct 27  
(c) 2004 The Dialog Corp.

Set	Items	Description
-----		
?s	CMEA or cellular (1n) message (1n) encryption	
	2808	CMEA
	1405480	CELLULAR
	953855	MESSAGE
	202517	ENCRYPTION
	70	CELLULAR(1N)MESSAGE(1N)ENCRYPTION
S1	2819	CMEA OR CELLULAR (1N) MESSAGE (1N) ENCRYPTION
?s	permut? (s) offset?	
	70872	PERMUT?
	755421	OFFSET?
S2	83	PERMUT? (S) OFFSET?
?s	lookup or mapping or map? or array?	
	26871	LOOKUP
	665464	MAPPING
	1930363	MAP?
	1302493	ARRAY?
S3	3184141	LOOKUP OR MAPPING OR MAP? OR ARRAY?
?s	(message or file? or data? or information) (3n) transform?)	
>>>Unmatched parentheses		
?s	(message or file? or data or information) (3n) (transform?)	
Processing		
Processed 10 of 27 files ...		
Processing		
Processed 20 of 27 files ...		
Processing		
Completed processing all files		
	953855	MESSAGE
	3152944	FILE?
	14015250	DATA
	17283802	INFORMATION
	2826933	TRANSFORM?
S4	91939	(MESSAGE OR FILE? OR DATA OR INFORMATION) (3N)
		(TRANSFORM?)
?s	s4 and s1	
	91939	S4
	2819	S1
S5	4	S4 AND S1
?s	(multiple? or plural? or many or second) (3n) (transform?) and s2	
Processing		
Processed 10 of 27 files ...		
Completed processing all files		
	3683844	MULTIPLE?
	50604	PLURAL?
	8296422	MANY
	6583986	SECOND
	2826933	TRANSFORM?
	27242	((MULTIPLE? OR PLURAL?) OR MANY) OR
		SECOND) (3N) TRANSFORM?
	83	S2
S6	3	(MULTIPLE? OR PLURAL? OR MANY OR SECOND) (3N)
		(TRANSFORM?) AND S2
?e	au=etzel,mark	

Ref	Items	Index-term
E1	1	AU=ETZEL, Z.
E2	2	AU=ETZEL, ZONGYIN
E3	0	*AU=ETZEL, MARK
E4	6	AU=ETZELL B M
E5	5	AU=ETZELL BM
E6	11	AU=ETZELL J
E7	2	AU=ETZELL J E
E8	7	AU=ETZELL JE
E9	2	AU=ETZELL JOAN
E10	1	AU=ETZELL JOAN E
E11	5	AU=ETZELL P

E12 7 AU=ETZELL P S

Enter P or PAGE for more  
?e au=frank,robert

Ref	Items	Index-term
E1	0	*AU=FRANK, ROBERT
E2	1	AU=FRANK, TRACYD
E3	1	AU=FRANKA
E4	2	AU=FRANKA G M
E5	1	AU=FRANKA J
E6	1	AU=FRANKA MR
E7	3	AU=FRANKA R
E8	2	AU=FRANKA S
E9	3	AU=FRANKA, J.
E10	5	AU=FRANKA, JOHN
E11	2	AU=FRANKA, S.
E12	2	AU=FRANKA, STEVE

Enter P or PAGE for more  
?e au= heer, daniel

Ref	Items	Index-term
E1	0	*AU=HEER, DANIEL
E2	2	AU=HEER, DANIEL N.
E3	1	AU=HEER, DARVIN
E4	2	AU=HEER, DAVID J.
E5	1	AU=HEER, DAVID M
E6	1	AU=HEER, DAVID M.
E7	1	AU=HEER, DAVID MACALPINE
E8	1	AU=HEER, DON
E9	3	AU=HEER, DONALD
E10	135	AU=HEER, E.
E11	13	AU=HEER, EWALD
E12	2	AU=HEER, EWALD (ED. )

Enter P or PAGE for more  
?e au=mxnelis,robert

Ref	Items	Index-term
E1	1	AU=MXLERoy, E.G.
E2	2	AU=MXN, JULIAN
E3	0	*AU=MXNELIS, ROBERT
E4	1	AU=MXOTKOWSKA B
E5	1	AU=MXQLLER, ANDERS PAPE
E6	1	AU=MXSKIMIN, H. J.
E7	3	AU=MY
E8	1	AU=MY ABDELMAJID KASSEM
E9	1	AU=MY AHMED IRAGI
E10	1	AU=MY AHMED MALIKI
E11	1	AU=MY AHMED SAID A S
E12	5	AU=MY AHMED SAID AZIZI SAMIR

Enter P or PAGE for more  
?e au=mcnelis,robert

Ref	Items	Index-term
E1	2	AU=MCNELIS, ROSEMARY HATTRUP
E2	1	AU=MCNELIS, WILLIAM J.
E3	0	*AU=MCNELIS, ROBERT
E4	2	AU=MCNELL B J
E5	1	AU=MCNELL H
E6	1	AU=MCNELL J J
E7	1	AU=MCNELL M
E8	1	AU=MCNELL N
E9	1	AU=MCNELL P L
E10	1	AU=MCNELL S E

E11 1 AU=MCNELL T F  
E12 1 AU=MCNELL, B.W.J.

Enter P or PAGE for more  
?e au=mizjkovsky,semyon

Ref	Items	Index-term
E1	0	*AU=MIZJKOVSKY,SEMYON
E2	1	AU=MIZKAN AI
E3	1	AU=MIZKAT H J
E4	1	AU=MIZKEWIC A N
E5	1	AU=MIZKJEWITSCH, N. V.
E6	1	AU=MIZKJEWITSCH, NIKOLAJ
E7	2	AU=MIZLA P
E8	1	AU=MIZLA, W. A.
E9	1	AU=MIZLER M O
E10	1	AU=MIZLIKOSHI K
E11	1	AU=MIZLO J
E12	1	AU=MIZLO, J.J., III

Enter P or PAGE for more  
?e au=rance,robert

Ref	Items	Index-term
E1	2	AU=RANCE, W. G.
E2	2	AU=RANCE, W.G.
E3	0	*AU=RANCE,ROBERT
E4	2	AU=RANCEA A
E5	1	AU=RANCEA G
E6	1	AU=RANCEA, GH.
E7	8	AU=RANCEL A
E8	1	AU=RANCEL C
E9	1	AU=RANCEL D M
E10	2	AU=RANCEL MMS
E11	3	AU=RANCEL N
E12	1	AU=RANCEL TORRES N

Enter P or PAGE for more  
?e au=shipp,R

Ref	Items	Index-term
E1	5	AU=SHIPP, WILLIAM S.
E2	1	AU=SHIPP, WILLIAM STANLEY
E3	0	*AU=SHIPP,R
E4	1	AU=SHIPPAM C
E5	1	AU=SHIPPAM CE
E6	1	AU=SHIPPAM G K
E7	1	AU=SHIPPAM J
E8	1	AU=SHIPPAM-BRETT C
E9	1	AU=SHIPPAM-BRETT CE
E10	1	AU=SHIPPAM, CYNTHIA ELIZABETH
E11	1	AU=SHIPPAN R
E12	1	AU=SHIPPAN, R.

Enter P or PAGE for more  
?s s3 and s2

3184141	S3
83	S2
S7 21	S3 AND S2

?s s4 and s3

91939	S4
3184141	S3
S8 15264	S4 AND S3

?s s8 and s1

15264	S8
2819	S1
S9 0	S8 AND S1

Google

[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

## CMEA and block cipher

## Search

### Advanced Search Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

## Web

Results 1 - 10 of about 456 for CMEA and block cipher. (0.60 seconds)

## Block cipher - Wikipedia, the free encyclopedia

**Block cipher.** ... In cryptography, a **block cipher** is a type of symmetric key cipher which operates on groups of bits of a fixed length, termed **blocks**. ...

[en.wikipedia.org/wiki/Block\\_cipher](https://en.wikipedia.org/wiki/Block_cipher) - 23k - [Cached](#) - [Similar pages](#)

Block cipher modes of operation - Wikipedia, the free encyclopedia

**Block cipher** modes of operation. From ... encyclopedia. In cryptography, a **block cipher** operates on **blocks** of fixed length, often 64 or 128 bits. ...

[en.wikipedia.org/wiki/Block\\_cipher\\_modes\\_of\\_operation](https://en.wikipedia.org/wiki/Block_cipher_modes_of_operation) - 23k - Cached - Similar pages

[ More results from en.wikipedia.org ]

**CMEA (cipher)** - encyclopedia article about **CMEA (cipher)**. Free ...

... | CMEA In cryptography, the Cellular Message Encryption Algorithm (CMEA) is a **block cipher** which was used for securing mobile phones in the United States. ...

encyclopedia.thefreedictionary.com/CMEA%20(cipher) - 41k - Cached - Similar pages

## Science Fair Projects - Cellular Message Encryption Algorithm

... In cryptography, the Cellular Message Encryption Algorithm (CMEA) is a **block cipher** which was used for securing mobile phones in the United States. ...

[www.all-science-fair-projects.com/science\\_fair\\_projects\\_encyclopedia/CMEA \(cipher\)-18k-Cached-Similar-pages](http://www.all-science-fair-projects.com/science_fair_projects_encyclopedia/CMEA_(cipher)-18k-Cached-Similar-pages)

**Block cipher - free-definition.com**

Search: **Block cipher**. Definition, Meaning, Explanation. In cryptography ... bits. 64-bit **blocks** became common in **block cipher** designs after DES. Key ...

www.free-definition.com/Block-cipher.html - 23k - Cached - Similar pages

## Kremlin. Cryptographic Algorithms

... It is a stream **cipher** based on three 32-bit Galois LFSRs. It is distinct from **CMEA**, which is a **block cipher** used to encrypt the cellular data control channel. ...

kremlinencrypt.com/algorithms.htm - 48k - Cached - Similar pages

Citations: Decrypting the Puzzle Palace - Barlow (ResearchIndex)

... CMEA (Control Message Encryption Algorithm) a simple **block cipher**, is used to encrypt the control channel [Ree91] The voice privacy algorithms has long been ...

[citeseer.ist.psu.edu/context/441837/0](https://citeseer.ist.psu.edu/context/441837/0) - 12k - Supplemental Result - Cached - Similar pages

```
[PS] [ ProductName: GNU Ghostscript ]
```

File Format: Adobe PostScript - View as Text

... I'Control channel uses **CMEA**, a variable. -width. **block cipher** with 2 rounds %%(Page: 26)%% Cryptanalysis!Voice privacy is XOR with 520 -bit mask. ...

[www.cs.berkeley.edu/~daw/talks/SAC02.ps](http://www.cs.berkeley.edu/~daw/talks/SAC02.ps) - Similar pages

## Cryptanalysis of the Cellular Message Encryption Algorithm

... 2 A description of **CMEA**. We describe the **CMEA** specification fully here for reference.

CMEA is a byte-oriented variable-width **block cipher** with a 64 bit key. ...

www.cs.berkeley.edu/~daw/papers/cmea-crypto97-www/paper10.html - 46k - Cached - Similar pages

[ More results from [www.cs.berkeley.edu](http://www.cs.berkeley.edu) ]

### Block cipher - Definition of Block cipher by Webster's Online ...

... 3-Way, AES, Blowfish, Camellia, CAST-128, CAST-256, CMEA, DEAL, DES, DES-X, FEAL, GDES, GOST, IDEA, Iraqi **block cipher**, KASUMI, Khafre, KHAZAD, Khufu, LOKI89/91 ...

www.webster-dictionary.org/definition/block%20cipher - 18k - Cached - Similar pages

Digitized by Google

1 2 3 4 5 6 7 8 9 10

# h g g e c e c h h e

b c c he b e ch